IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re Dealer Management Systems Antitrust Litigation, MDL 2817	No. 1:18-CV-864
This document relates to: *Authenticom, Inc. v. CDK Global, LLC et al.*, Case No. 1:18-cv-00868 (N.D. Ill.)	Hon. Robert M. Dow, Jr. Magistrate Judge Jeffrey T. Gilbert

COUNTERCLAIMANT THE REYNOLDS AND REYNOLDS COMPANY'S [PROPOSED] MEMORANDUM IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Because there is no genuine issue of material fact regarding threshold liability issues, Counterclaimant The Reynolds and Reynolds Company ("Reynolds") brings this Motion for Partial Summary Judgment in favor of certain of its counterclaims against Counterclaim-Defendant Authenticom, Inc. ("Authenticom") pursuant to Federal Rule of Civil Procedure 56 in order to streamline and narrow the issues in dispute in this litigation.

I. Introduction

Reynolds owns and operates an enterprise computing system that it protects from unauthorized intrusion by numerous technological methods. Since at least 2009, Authenticom has engaged in a persistent campaign to solicit and use credentials meant solely for licensed users of Reynolds's system and to circumvent Reynolds's technological access-control measures. Authenticom's circumvention efforts included using Eastern European CAPTCHA farms, input spoofing, illegal copying of copyrighted software, various measures intended to conceal its actions on the Reynolds system, and other hostile system attacks. Long before Authenticom brought its retaliatory antitrust claims, Reynolds demanded that Authenticom cease and desist from its illegal hacking of Reynolds's system and offered Authenticom an orderly wind down of its unlawful activities. Authenticom refused. Instead, even though legal alternative methods of obtaining dealers' operational data were available to it, Authenticom chose expediency over legality and elected to persist in its unlawful practices. Authenticom's data-extraction business with respect to Reynolds's system is, based on uncontroverted material facts established in discovery, illegal as a matter of law. Accordingly, Reynolds seeks partial summary judgment as to Authenticom's liability on Reynolds's counterclaims under (1) the Digital Millennium Copyright Act ("DMCA") and (2) the Wisconsin Computer Crimes Act ("Computer Crimes Act").

Fact discovery is now closed, and the material facts establishing Authenticom's liability under these two statutes are not disputed—nor is any expert discovery needed to resolve this

motion. Partial summary judgment on these narrow liability issues (as contrasted with the magnitude of that liability—i.e., how many times Authenticom utilized its illegal methods or otherwise engaged in illegal conduct and resulting damages) is appropriate at this time and will aid in resolving this litigation efficiently and expeditiously.

II. Statement of Undisputed Facts

Pursuant to Local Rule 56.1, the undisputed facts in support of this motion are set forth in Reynolds's accompanying Statement of Undisputed Material Facts.

III. Legal Standard

Under Rule 56, summary judgment is appropriate when the movant can show there are no genuine disputes of material fact and the movant is entitled to judgement as a matter of law. Fed. R. Civ. P. 56(a). The Seventh Circuit and this Court encourage the use of early summary judgment motions to simplify disputes and reduce litigation costs. *See, e.g.*, *S. Austin Coalition Cmty. Council v. SBC Commc'ns, Inc.*, 274 F.3d 1168, 1171 (7th Cir. 2001); *Johnke v. Espinal-Quiroz*, 14-CV-6992, 2018 WL 3361888, at *3 (N.D. Ill. July 9, 2018).

IV. Applicable Limitations Periods

The DMCA's limitations period is three years, subject to discovery-rule tolling. 7 U.S.C. § 507; *Chicago Bldg. Design, P.C. v. Mongolian House, Inc.*, 770 F.3d 610, 614 (7th Cir. 2014). Wisconsin does not provide an explicit statute of limitations for civil actions under the Computer Crimes Act. However, the statute of limitations for prosecution of felony violations of that statute is six years. Wis. Stat. § 939.74(a). That six-year period mirrors the Wisconsin limitations period for civil actions for fraud, Wis. Stat. § 893.93(1)(b), and trespass, § 893.52(1)—causes of action fundamentally similar to the civil Computer Crimes Act claim.

Reynolds's DMCA and Computer Crimes Act counterclaims are compulsory and therefore relate back to May 1, 2017, the date on which Authenticom filed its complaint. *Seitz v. Beeter*,

2013 WL 409428, at *2 (N.D. Ill. Jan. 31, 2013) (collecting cases). Reynolds's DMCA claim accordingly runs back to (at minimum) May 1, 2014, and its Computer Crimes Act claim runs back to May 1, 2011.

Counterclaims are compulsory when they arise from the same transaction or occurrence that is the subject of the plaintiff's claim. Fed. R. Civ. P. 13(a)(1)(A). A counterclaim arises from the same transaction or occurrence when it is "logically related" to the plaintiff's claim. *E.g.*, *Burlington N. R.R. Co. v. Strong*, 907 F.2d 707, 711 (7th Cir. 1990). "There is no formalistic test to determine whether the claims are logically related." *In re Price*, 42 F.3d 1068, 1073 (7th Cir. 1994). Instead, courts consider "the totality of the claims, including the nature of the claims, the legal basis for recovery, the law involved, and the respective factual backgrounds." *Burlington Northern*, 907 F.2d at 711.

Reynolds's counterclaims are compulsory under that standard. The claims and counterclaims stem from the same course of conduct on both sides: Reynolds's efforts to prevent unauthorized third parties from accessing the Reynolds DMS, and Authenticom's efforts to defeat (and alleged harm from) Reynolds's prevention measures. Authenticom alleges that Reynolds improperly "blocked" and "disabled" Authenticom's access to and use of the Reynolds DMS through escalating technological blockades, harming Authenticom's business and requiring it to develop technological workarounds.[1] Reynolds alleges, on the other hand, that it was entitled by law to control access to its proprietary and copyrighted software platform through licensing agreements and technological access controls in the first instance, and that Authenticom's efforts to circumvent those agreements and controls were unlawful.[2] Courts routinely hold that competing antitrust and intellectual-property claims of this nature are "logically related" and thus

[1] *See, e.g.*, Auth. Compl. [Auth. Dkt. 1] ¶¶ 6, 12, 74, 92, 103, 106-107, 109, 121, 185, 189.
[2] *See* Reynolds Answer and Counterclaims [Dkt. 225] ¶¶ 2, 8-13, 30-32, 49-64, 67-80, 125-135.

compulsory.[3]

Like the antitrust plaintiffs in the seminal case establishing the logical relationship test, (*Moore v. New York Cotton Exchange*, 270 U.S. 593 (1926)[4]), Authenticom resorted to a pincer strategy of antitrust litigation and hook-or-crook self-help. Reynolds responded with counterclaims asserting that Authenticom's self-help was unlawful in the first place. Reynolds's refusal to provide Authenticom with access to and use of the Reynolds DMS "is one of the links in the chain which constitutes the transaction upon which" Authenticom "bases its cause of action," and without that refusal "neither party would have found it necessary to seek relief." *See id.* Thus, like the New York Cotton Exchange's claims in *Moore*, Reynolds's counterclaims are compulsory notwithstanding that the facts and legal issues "are not precisely identical, or that the counterclaim embraces additional allegations, as, for example, that" Authenticom "is unlawfully getting" access to and use of the Reynolds DMS.[5] *See id.*

V. Partial Summary Judgment Is Appropriate Regarding Authenticom's Liability for Certain Counterclaims

A. Authenticom Violated the DMCA's Anti-Circumvention Provision.

Authenticom's efforts to force access to the Reynolds DMS violated the DMCA's anti-circumvention provision as a matter of law. As part of its data polling processes, Authenticom

[3] *See, e.g.*, *Critical-Vac Filtration Corp. v. Minuteman Int'l, Inc.*, 233 F.3d 697, 700 (2d Cir. 2000) (applying logical relationship test to hold that antitrust claims were compulsory counterclaims to earlier patent infringement action); *Rohm & Haas Co. v. Brotech Corp.*, 770 F. Supp. 928, 930–31 (D. Del. 1991) (applying logical relationship test to hold that antitrust claims were compulsory counterclaims to patent infringement action and collecting cases); *Harley-Davidson Motor Co. v. Chrome Specialties, Inc.*, 173 F.R.D. 250, 252 (E.D. Wis. 1997) (applying logical relationship test to hold that antitrust claim was compulsory counterclaim to trademark infringement claim); *Grumman Sys. Support Corp. v. Data Gen. Corp.*, 125 F.R.D. 160, 162–63 (N.D. Cal. 1988) (applying logical relationship test to hold that antitrust claim was compulsory counterclaim to copyright claim).

[4] *See* WRIGHT & MILLER, 6 FED. PRAC. & PROC. CIV. § 1410 (3d ed.) (describing *Moore* as "the leading Supreme Court case on compulsory counterclaims").

[5] This Court's holding regarding limitations of CDK's counterclaims in the Dealer Class case (Dkt. 749) is distinguishable as Authenticom's complaint is based on a theory of blocking. *See, e.g.*, Auth. Compl. [Auth. Dkt. 1] ¶¶ 6, 12, 74, 92, 103, 106-107, 109, 121, 185, 189. Further, in *Moore* the Supreme Court expressly rejected a narrow test, holding that it "does not matter" that the counterclaim encompassed "additional allegations" like the unlawfulness of the counterclaim-defendant's actions in acquiring the disputed data. *Moore*, 270 U.S. at 609-10.

developed and used several technological measures that served this express purpose. Authenticom does not dispute the basic functionality of these measures—i.e., what they did technically. Nor does Authenticom dispute their intended purpose—i.e., why they were designed and implemented. Instead, Authenticom repeatedly resorts to overgeneralized euphemisms—contending that it used such expedient hostile measures to "keep the data flowing"—or justifying its actions based on supposed authorization from dealers. But as set forth below, neither of those contentions matter.

Section 1201(a)(1)(A) of the DMCA prohibits circumvention of access controls: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." The DMCA defines "circumvent a technological measure" to mean "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." *Id.* at § 1201(a)(3)(A). The DMCA further defines the phrase "circumvent protection afforded by a technological measure" to mean "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure." *Id.* at § 1201(b)(2)(A).

Authenticom repeatedly violated the DMCA's anti-circumvention provision (§ 1201(a)(1)(A))[6] with respect to the Reynolds DMS. As Authenticom's Chief Executive Officer, Steve Cottrell, testified in the Wisconsin injunction hearing:

> Q The status quo as it relates to Reynolds from 2010 to 2017 has been that Reynolds is actively blocking Authenticom and Authenticom does what it can to **get around those blocks**; right?
>
> A Yes. I would say that's correct, yes.[7]

[6] Reynolds is only seeking summary judgment as to this subsection of the DMCA. Reynolds has other DMCA claims against Authenticom that it intends to present at trial.
[7] Auth. P.I. Tr. 1-P [Auth. Dkt. 162] at 44:10-14 (Testimony of S. Cottrell) (emphasis added).

Authenticom has expressly bragged about its circumvention efforts, announcing as recently as 2017 that it was "[redacted]."[8] Indeed, before Reynolds filed its counterclaims, Authenticom confessed in this lawsuit that it had worked to "develop **workaround solutions** that **circumvented** Reynolds's efforts to block access." Mot. for P.I. at 8 [Dkt. 61] (emphasis added); *see also* Auth. 7th Cir. Resp. Br. at 12 ("Reynolds' efforts, however, were not entirely successful; Authenticom, CDK, and other integrators worked with dealers to develop **workarounds**."). In the Authenticom chart below,[9] Authenticom itself laid out how it targeted Reynolds's access controls with hostile "resulting" actions:

[redacted]

[8] Ex. 99, AUTH_00280842, at 845 (emphasis added). [redacted]uthenticom witness Katie Wiersgalla confirmed [redacted]. *See* Ex. 24 at 225:12-15 (Wiersgalla tr.).

[9] *See* Ex. 26, AUTH_00468320.

As illustrated in the chart above (and detailed in the accompanying Statement of Undisputed Facts), Authenticom's attempts to access the Reynolds DMS without Reynolds's authorization were flagrant, prolific, and continued in various forms from at least 2009 to the present.[10] Just one of the "technologies" Authenticom used to crack into Reynolds's system was its well-documented use of CAPTCHA circumvention methods.[11] This Court has already found that Authenticom's use of automated tools and CAPTCHA farms to respond to CDK's CAPTCHA prompts falls within the DMCA's prohibition. Order at 17 [Dkt. 506]. The Court further held that Authenticom's implementation of a software tool that automatically reenabled disabled user IDs supported DMCA liability. *Id.* Authenticom's attacks on the Reynolds system—through CAPTCHA cracking and other methods—were even more relentless.

1. The Reynolds DMS is protected by the Copyright Act.

As an initial matter, the DMCA applies in connection with "works protected under this chapter"—i.e., the copyright laws of the United States. 17 U.S.C. §§ 1201(a)(1), (a)(2), (b)(1). That element is not disputed here. "[A]lmost all novel software code constitutes a creative, original work of authorship that is automatically protected under the Copyright Act." *Synopsys, Inc. v. AzurEngine Techs., Inc.*, 19CV1443-LAB (AGS), 2019 WL 3842996, at *2 (S.D. Cal. Aug. 15, 2019). The Reynolds DMS is such an original copyrighted work.[12] Components of the Reynolds DMS are also protected by registered copyrights, including ERAccess.exe and ERA-

[10] Unlike all the other entries in this chart, Authenticom's use of "[redacted]" was not a DMCA violation—instead, it was the legitimate course of action that Authenticom should have taken all along. [redacted] *See, e.g.*, Ex. 24 at 70:10-19 (Wiersgalla tr.).

[11] *See, e.g.*, Ex. 45 at 79:18-19 (Robinson tr.) ("[redacted]."); *see also infra*.

[12] Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 14 (Testimony of R. Schaefer); Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 4, 14, 27; Ex. 13.

IGNITE.exe.[13] ERAccess and ERA-IGNITE are PC software applications that dealer employees use under a license from Reynolds to access and operate the Reynolds DMS—and that Authenticom [redacted].[14] The copyright registrations for those specific components of the DMS are prima facie evidence of validity, and Authenticom has adduced no evidence to challenge them. *See* 17 U.S.C. 410(c). And although Reynolds has not *registered* copyrights on other components of the DMS, all Reynolds DMS software is still *protected* by copyright as "copyright automatically inheres in the work at the moment it is created without regard to whether it is ever registered." *Montgomery v. Noga*, 168 F.3d 1282, 1288 (11th Cir. 1999).

2. Authenticom circumvented access controls in the Reynolds DMS.

The Reynolds DMS contains multiple access controls intended to protect its copyrighted contents. For purposes of the DMCA's Section 1201(a), "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). As summarized by the *Authenticom* court in Wisconsin:

> Reynolds began blocking Authenticom's access to its DMS in 2009, and it achieved more effective blocking around 2013, apparently by using technology that was able to detect and instantly disconnect automated access to its DMS.

Authenticom, Inc. v. CDK Glob., LLC, 17-CV-318-JDP, 2017 WL 3017048, at *3 (W.D. Wis. July 14, 2017), vacated, 874 F.3d 1019 (7th Cir. 2017).

[13] Ex. 9 (Copyright TX 7-586-896); Ex. 10 (Copyright TX 7-586-863); Ex. 11 (Copyright TX 8-538-825); Ex. 12 (Copyright TX 8-538-541). The Court may properly take judicial notice of these registrations. *See Brooks-Ngwenya v. Indianapolis Pub. Schools*, 564 F.3d 804, 808 (7th Cir. 2009) (taking judicial notice of copyright registration).
[14] *See, e.g.*, Ex. 39 at 35:6-13 (Munns tr.); Ex. 2 at 63:22-64:2 (Kirby tr.); Ex. 14, REYMDL00022920 (Aug. 19, 2010 ERAccess announcement); Ex. 15, REYMDL00022918 (Jan. 14, 2011 ERAccess announcement); Ex. 1 at 34:3-16, 94:3-25 (Burnett tr.) (discussing ERA and ERA-IGNITE).

Reynolds files this motion with respect to two access controls in particular: 1) Reynolds's CAPTCHA prompts; and 2) Reynolds's "Suspicious User ID" detection program that was designed to detect automated user accounts and flag them for deactivation.[15] Both of these methods were developed and implemented by Reynolds before any alleged conspiracy with CDK. And as described below, both were subject to persistent, deliberate, and illegal circumvention efforts by Authenticom.

a. Authenticom circumvented Reynolds's CAPTCHA controls via automated methods and CAPTCHA farms.

CAPTCHA is an acronym for "Completely Automated Public Turing Test to tell Computers and Humans Apart."[16] As the name indicates, the purpose of a CAPTCHA prompt is to prevent automated access to a computer system or software.[17] CAPTCHA functions by displaying an image, characters, or other question that a human can readily answer and a machine cannot.[18] CAPTCHA prompts are a well-recognized form of access control measure under the DMCA.[19] Indeed, this Court has already held that CDK's CAPTCHA prompts constitute such a measure. Order at 17-18 [Dkt. 506]. The same applies with equal force and effect to Reynolds.

Reynolds implemented several different forms of CAPTCHA prompts within its DMS. In 2009, Reynolds began requiring users to answer "Challenge Questions," which were intended to be answerable only by humans (e.g., "What color is the sky?").[20] In 2010, Reynolds introduced

[15] This list is not exhaustive; instead, it is targeted at the two most flagrant examples of Authenticom's circumvention for which there are no material disputed facts. Reynolds reserves all rights regarding other acts of circumvention and other access controls.
[16] *Craigslist, Inc. v. Kerbel*, C-11-3309 EMC, 2012 WL 3166798, at *1 n.2 (N.D. Cal. Aug. 2, 2012).
[17] *Id.* at *1; Ex. 16 at 64:23-65:6 (Lamb tr.).
[18] *See* Ex. 16 at 64:23-65:6 (Lamb tr.); *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1112 (C.D. Cal. 2007) (describing CAPTCHA functionality).
[19] *See, e.g.*, *id.*; *Ticketmaster L.L.C. v. Prestige Entm't, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018); *see also Ticketmaster L.L.C. v. Prestige Entm't W., Inc.*, 315 F. Supp. 3d 1147, 1167 (C.D. Cal. 2018) ("The Court's finding falls in line with the growing number of courts that have concluded that circumvention of CAPTCHA and similar measures designed to distinguish between humans and non-humans violates the DMCA.").
[20] Ex. 20, REYMDL00015519; Ex. 26, AUTH_00468320 (Authenticom timeline chart); Ex. 28 at 46:14-17 (Clements tr.) (describing Reynolds challenge questions); Declaration of S. Cottrell [Auth. Dkt. 51] ¶ 37.

ASCII Captchas, a form of CAPTCHA adapted for the green-screen terminals in use at the time.[21] And in 2012, Reynolds replaced ASCII with graphical CAPTCHAs, the widely adopted form of CAPTCHA found throughout modern websites and computer systems.[22]

Authenticom circumvented these measures in several ways. One was [redacted].[23] [redacted].[24] That method plainly violates the DMCA's anti-circumvention prohibition. *See* Order at 17-18 [Dkt. 506]; *Ticketmaster*, 306 F. Supp. 3d at 1174. Indeed, multiple Authenticom witnesses testified that this method was [redacted],[25] yet as of February 26, 2014, Authenticom was [redacted].[26]

Authenticom also utilized CAPTCHA farms to answer Reynolds's CAPTCHA prompts. Authenticom's data extraction software would [redacted][27] [redacted]

[21] Ex. 20, REYMDL00015519; Ex. 26, AUTH_00468320; Ex. 28 at 48:13-24 (Clements tr.) (describing Reynolds ASCII CAPTCHAs).
[22] *See* Ex. 26, AUTH_468320; Ex. 20, REYMDL00015519; *see generally* Ex. 16 at 65:7-17 (Lamb tr.) (describing Reynolds's long history of CAPTCHA use); Ex. 29 at 172:7-11 (Cottrell 2019 tr.) ("[redacted]."); Authenticom Resp. to Defs. Statement of Add'l Facts [Auth. Dkt. 145] (hereinafter "Auth. Resp. to DSAF") ¶¶ 75, 76 ("Undisputed that Reynolds implemented a series of roadblocks to prevent dealers from using independent integrators, including challenge questions and captcha."); Authenticom Compl. [Auth. Dkt. 1] ¶ 189 (admitting that Reynolds introduced Challenge Questions and CAPTCHA in 2009, which were intended "to make it more difficult to automate the pulling of data").
[23] *See* Ex. 29 at 268:12-22 (Cottrell 2019 tr.) ("[redacted]"); Ex. 45 at 77:5-10, 80:9-11 (Robinson tr.) (Authenticom developed "[redacted]"); .
[24] Ex. 39 at 140:4-5 (Munns tr.); Ex. 46, AUTH_00096097. [redacted] Ex. 39 at 148:11-149:19 (Munns tr.); Ex. 49, AUTH_00091915. *See also, e.g.*, Ex. 100, AUTH_00094640 [redacted]").
[25] *See, e.g.*, Ex. 39, 152:3-7 (Munns tr.).
[26] *See* Ex. 49, AUTH_00083390.
[27] *See* Ex. 33, AUTH_00141204 (Authenticom would [redacted]).

[redacted]"[28] [redacted].[29] Authenticom was thereby able to thwart Reynolds's CAPTCHA-based efforts to prevent automated access to its system. Indeed, Authenticom's documents indicate [redacted].[30] Authenticom previously argued that such methods do not violate the DMCA, but the Court correctly rejected that contention. *See* Order at 17-18 [Dkt. 506]. Other courts have as well. *See Ticketmaster*, 306 F. Supp. 3d at 1174. Authenticom's use of CAPTCHA farms—combined with the Authenticom software that leveraged them—falls squarely within the DMCA's prohibition.

Discovery uncovered several other Authenticom CAPTCHA cracking methods as well, none of which were authorized by Reynolds. The first was [redacted].[31] The second was [redacted].[32] And the third was [redacted]"[33] [redacted].[34] These methods all violate the DMCA under the same logic and reasoning set forth above and in the Court's Order on the CDK counterclaims.

[28] *See, e.g.*, Exs. 50-64, 82 (receipts for Death by CAPTCHA services); Def. Ex. 6 (Death by CAPTCHA website).
[29] *See* Ex. 33, AUTH_00141204; Ex. 28 at 138:5-16 (Clements tr.).
[30] *See, e.g.*, Exs. 50-64, 82 (receipts for Death by CAPTCHA services); Ex. 65 at 79:19-88:9 (Noth tr.).
[31] Ex. 40 at 172:3-22 (Authenticom 30(b)(6) Brown tr.).
[32] *Id.* at 170:15-171:16, 172:3-22 (Authenticom 30(b)(6) Brown tr.).
[33] *Id.* at 161:4-8 ("[redacted]").
[34] Ex. 46, AUTH_00096097; *see also, e.g.*, Ex. 67, AUTH_00092142 (discussing this process).

b. Authenticom circumvented Reynolds's security controls intended to detect and disable automated users in the DMS.

Reynolds is also entitled to summary judgment with regard to Authenticom's efforts to circumvent and avoid Reynolds's Suspicious User ID tracking process.

Security monitoring programs—particularly those looking for unauthorized automated processes—are another recognized form of access control measure. For example, in *MDY Industries LLC v. Blizzard Entertainment, Inc.*, the Ninth Circuit examined a system implemented by Blizzard Entertainment that was intended to detect the use of automated "bots" by users in the "World of Warcraft" online computer game. 629 F.3d 928 (9th Cir. 2010). The detection system, nicknamed "Warden," was designed to check users' computers for "patterns of code associated with known bots or cheats." *MDY*, 629 F.3d at 942. If such a pattern was detected, the user would be disabled. *Id.* The Ninth Circuit held that this constituted an access control measure under the DMCA. *Id.* at 954.

Similarly, one district court analyzed a measure called "HackShield," which was another process intended to prevent automated processes in a video game. As described by the court, "if HackShield detects unauthorized processes or data, HackShield sends a message to Combat Arms [the game at issue] to stop operating, at which point the game forcibly will close." *Nexon Am., Inc. v. Game Anarchy, LLC*, CV-12-02083-MWF (PLAX), 2013 WL 12121539, at *2 (C.D. Cal. Apr. 3, 2013). The court granted judgment as a matter of law on a DMCA claim for evasion of this measure. *Id.* As both these cases further make clear, the fact that an offender may be able to circumvent a control is not disqualifying: "[t]he statutory definition of the phrase 'effectively control access to a work' does not require that an access control measure be strong or circumvention-proof." *MDY*, 629 F.3d at 954 n.17. So long as the measure provides "some degree of control over access to a copyrighted work," the standard is satisfied. *Id.*

Reynolds's Suspicious User ID system is similar in key respects. On August 8, 2011, Reynolds announced: "[redacted]."[35] This release contained [redacted].[36] Those monitoring attempts culminated in the Suspicious User ID process. As described in the user guide for Reynolds's May 2013 software update:

[redacted][37]

This Suspicious User ID process, which Reynolds has continued to refine over time, was included in all versions of Reynolds's ERA DMS released from May 2013 forward.[38]

Reynolds's monitoring process [redacted].[39] [redacted].[40]

[35] Ex. 31, REYMDL00022904 (August 8, 2011 Reynolds System Announcement); Ex. 93, REYMDL00015727 (Authenticom receipt of same on August 11, 2011); Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 6-7, 9 (describing ERA).
[36] *See* Ex. 31, REYMDL00022904.
[37] Ex. 30, REYMDL00001971, at 1976; *see also id.* at 1977 ("When the User ID attempts to access the ERA® System with software or a communications method not supported by Reynolds and Reynolds, the User ID is immediately disabled.").
[38] *See* Auth. Resp. to DSAF [Auth. Dkt. 145] ¶ 77; Declaration of R. Schaefer [Auth. Dkt. 97] ¶ 30.
[39] *See, e.g.*, Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 15, 16 (Testimony of R. Schaefer).
[40] *See, e.g.*, *id.*; Ex. 32, AUTH_00219452 (containing examples of disabled Authenticom IDs and associated screenshots from the Reynolds DMS).

Reynolds's Suspicious User ID program falls squarely within the DMCA's "access control" definition: it is intended to effectively control access to the DMS by identifying and disabling any accounts that appear to be automated. Stated in the language of the statute, it requires the application of information and processes that establish the account is being used by a human rather than automated user. 17 U.S.C. § 1201(a)(3)(B). Authenticom admits, as it must, that Reynolds's technological measures targeted automated access in particular and "aggressively identify[ed] and block[ed] suspicious user IDs" that it believed were being used by these unauthorized third parties.[41]

Authenticom's efforts to circumvent Reynolds's monitoring controls were pervasive and persistent. Some were [redacted].[42] Others were technological. For example, Authenticom [redacted]"[43] The goal of this script was "[redacted]"[44] Authenticom even resorted [redacted].[45]

Authenticom also modified its polling programs to [redacted]. As one Authenticom developer summarized:

[41] Auth. Resp. to DSAF [Auth. Dkt. 145] ¶ 77.
[42] *See, e.g.*, Ex. 69, AUTH_00168020 ("[redacted]"); Ex. 70, AUTH_00168116 ("[redacted]").
[43] Ex. 71, AUTH_00465304.
[44] Ex. 72, AUTH_00230422, at 5.
[45] *See* Ex. 77, AUTH_00221025; Ex. 78, AUTH_00091792.

[redacted].[46]

Trying to "get around" a security measure by "tricking" the system is the definition of a DMCA violation. The Reynolds system [redacted].[47] To avoid this control, Authenticom [redacted]."[48]

Authenticom extensively tested and refined its evasion measures. For example, Authenticom arrived at [redacted] after various other attempts to avoid detection.[49] In 2013, Authenticom [redacted].[50] Similarly, in May 2015, Authenticom [redacted]:

[redacted]

[46] Ex. 36, AUTH_00167914 (emphasis added).
[47] *See* Ex. 33, AUTH_00141204; Ex. 34, AUTH_00093108; Ex. 35, AUTH_00141219; Ex. 36, AUTH_00167914.
[48] Ex. 33, AUTH_00141204.
[49] *See, e.g.*, Ex. 36, AUTH_00167914; Ex. 79, AUTH_00170407; Ex. 35, AUTH_00141219.
[50] *See* Ex. 68, AUTH_00171450.

As indicated by the table,[51] Authenticom was [redacted].

Authenticom also worked to [redacted]. To extract data from a Reynolds DMS, Authenticom would [redacted].[52] Over time Authenticom became concerned that [redacted].[53] Authenticom eventually [redacted]"[54] Manipulating a computer's identifying criteria in this fashion is a recognized form of unlawful circumvention. *See, e.g.*, *Synopsys, Inc. v. InnoGrit, Corp.*, 19-CV-02082-LHK, 2019 WL 2617091, at *3 (N.D. Cal. June 26, 2019) (holding that changing the MAC addresses on computers to run unauthorized software is DMCA circumvention).

In short, from virtually the inception of Reynolds's measures to block or disable automated accounts, Authenticom utilized continuous efforts to avoid those measures. At a minimum, that included [redacted]. These are DMCA violations as a matter of law.

3. Authenticom's defenses for its circumvention activities fail.

There is no valid legal defense to Authenticom's DMCA violations. Authenticom's primary defense of its circumvention activities is to claim that it was "authorized" by the dealers

[51] Ex. 33, AUTH_00141204.
[52] *See* Ex. 39, 113:17-115:18 (Munns tr.); Ex. 34, AUTH_00093108 (stating that Authenticom was [redacted]).
[53] *See, e.g.*, Ex. 80, AUTH_00094637 (email chain re: "[redacted]"); Ex. 81, AUTH_00174085 ("[redacted]").
[54] Ex. 33, AUTH00141204.

to use them. For example, when Reynolds directly put this issue to Authenticom in a Request For Admission, Authenticom refused to answer by reframing the Request to mean "without dealer authorization."[55] Similarly, in response to a Reynolds Interrogatory, Authenticom answered:

.[56]

That is an admission of DMCA liability. The "dealer authorization" defense is a non-starter as a matter of law. The DMCA makes clear that any authorization must come from the copyright *owner*—which in this case is Reynolds alone. *See* 17 U.S.C. § 1201(a)(3) (defining circumvention as evading an access-control measure "without the authority of the copyright owner"). Reynolds does not authorize dealers to grant any third-party access to the Reynolds system.[57] Indeed, Judge Peterson found that "Reynolds has never approved of third-party access based solely on the *dealer*'s authorization."[58] The record is also replete with evidence that

[55] *See* Ex. 101, Authenticom Response to Reynolds Request for Admission No. 3.
[56] Ex. 102, Authenticom Answer to Reynolds Interrogatory No. 19.
[57] *See* Ex. 4, REYMDL00677044 (Reynolds Master Agreement) ("You agree . . . not to disclose or provide access to any Licensed Matter or non-public portions of the Site to any third party, except your employees who have a need for access to operate your business and who agree to comply with your obligations under this Section[.]"); Ex. 5, REYMDL00012246 (Reynolds Customer Guide) at 256 ("You agree that you and third parties acting on your behalf have no right or authority to access or audit Reynolds' systems, applications, processes, procedures, or practices, except to the extent specifically authorized by Reynolds."), at 265 ("Unless we provide otherwise, you may not install Other Matter on the Equipment or connect Other Matter to Licensed Matter, either directly or remotely, without our prior written consent."); at 267 ("You expressly acknowledge that the Licensed Matter constitutes valuable proprietary property, includes confidential information and constitutes trade secrets that embody substantial create efforts and that is valuable to Reynolds. You agree to keep confidential the Licensed Matter (including al licensed copies and Documentation) covered under the Documents and shall not copy, reproduce, distribute, or in any way disseminate or allow access to or by third parties."); *see also* Ex. 6, REYMDL00675678 (Defined Terms list); Ex. 94, REYMDL00676893 (Reynolds Authorization Letter).
[58] *Authenticom*, 2017 WL 3017048, at *2 (emphasis in original).

Authenticom was aware of this undisputed fact.[59] Any dealers' "authorization" is ineffective and legally irrelevant.[60]

Moreover, authorization to *access* a work is insufficient as a matter of law to establish authorization to *circumvent* an access control. "Even 'lawful purchasers' must establish that they had specific 'authorization to circumvent' in order to avoid DMCA liability." *Synopsys*, 2019 WL 3842996, at *2. Authenticom (which is neither a lawful purchaser nor licensee of the Reynolds DMS) cannot establish any such circumvention-specific authorization.[61] Moreover, this Court recently held that the dealers themselves are subject to DMCA liability for their circumvention efforts, *see* Order at 28 [Dkt. 749], which further undercuts any notion that dealers could immunize Authenticom's actions. There is no authorization-based defense to Authenticom's circumventions.

Authenticom's other stated excuse is that it was simply using the DMS in the same way as an ordinary authorized user, relying on this Court's opinion in *Navistar, Inc. v. New Baltimore Garage, Inc.*, 11-CV-6269, 2012 WL 4338816 (N.D. Ill. Sept. 20, 2012). But *Navistar*'s holding that one person can use another person's credentials without violating the DMCA is inapplicable here. The Court already correctly rejected that defense with regard to CAPTCHA circumvention. Order [Dkt. 506] at 17-18. Humans sharing an ID is categorically different than Authenticom's

[59] *See, e.g.*, Ex. 90, AUTH_00468019; Ex. 85 at 100:1-6; 128:14-16 (Gentry tr.) ("[redacted]"); Ex. 28 at 60:5-63:22 (Clements tr.) ([redacted]); Ex. 19, AUTH_00170940 ([redacted].").

[60] To the extent that Authenticom argues that Reynolds's provision of certain temporarily exempted user IDs precludes summary judgment, that argument fails too. The fact that Reynolds provided temporary, limited exceptions in some situations (e.g., transition period of an OEM switching from hostile "polling" to a Reynolds interface) never gave Authenticom blanket authorization to access the Reynolds system or circumvent access controls. Moreover, [redacted]. *See* Ex. 33, AUTH00141204. Thus, they fall outside the scope of this summary judgment motion and provide Authenticom with no defense to all the other instances where it *did* bypass Reynolds's CAPTCHA prompts and automated-access defenses.

[61] *See, e.g.*, Ex. 29 at 269:16-273:4 (Cottrell 2019 tr.) (admitting that [redacted]").

automated CAPTCHA-solving methods discussed above. A CAPTCHA prompt is designed to be answered by an individual dealership employee sitting at a DMS terminal. Authenticom's methods were designed to bypass that requirement through technological means.

This defense similarly does not apply to Authenticom's attempts to evade the Suspicious User ID control. No ordinary dealer employee user needs to resort to Menu Walk scripts, input spoofing, or serial number manipulation, precisely *because they are human* and their usage of the system does not trip anti-automation access controls. Pretending to be a human user to fool the system into granting system access does not immunize Authenticom from DMCA liability; instead, it establishes liability.

Authenticom does not dispute any of these facts regarding what its software did from a functional perspective—i.e., how it tried to avoid Reynolds's access controls. Instead, Authenticom witnesses characterized their attempts to avoid Reynolds's access controls as being intended to "[redacted]," or used other similar generalizations.[62] But the mere fact that Authenticom thought it was pursuing its business goals via its actions is no excuse. In other cases, the parties circumventing Ticketmaster's CAPTCHA prompts undoubtedly intended to keep the tickets flowing, and the parties circumventing Craigslist's controls intended to keep the Craigslist posts flowing. That did not spare those parties from DMCA liability. *See Craigslist*, 2012 WL 3166798, at *1; *Ticketmaster*, 306 F. Supp. 3d at 1174. It does not spare Authenticom either.

4. To the extent required, there was a "nexus" between Authenticom's circumventions and Reynolds's rights under the Copyright Act.

Though the DMCA does not, on its face, require a connection or nexus to an underlying copyright protection, courts are divided on this potential requirement. *Compare Chamberlain*

[62] Ex. 24 at 73:11-74:15 (Wiersgalla tr.); Ex. 29 at 269:16-270:1, 333:13-334:18 (Cottrell 2019 tr.); Ex. 40 at 161:21-162:1 (Authenticom 30(b)(6) Brown tr.).

Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1193 (Fed. Cir. 2004) (imposing such a nexus),[63] *with MDY Indus., LLC v. Blizzard Entm't, Inc.*, 629 F.3d 928, 950 (9th Cir. 2010) ("While we appreciate the policy considerations expressed by the Federal Circuit in *Chamberlain*, we are unable to follow its approach because it is contrary to the plain language of the statute."). The Seventh Circuit has not addressed this issue. But it makes no difference: Reynolds can readily satisfy the nexus here.

Reynolds implemented its access controls to prevent unlicensed third parties like Authenticom from copying and distributing Reynolds's proprietary software. Authenticom engaged in such acts of copying repeatedly and flagrantly, thereby violating (or at least implicating) Reynolds's rights under the Copyright Act. *See* 17 U.S.C. 106. Indeed, Authenticom witnesses admitted that throughout the relevant time period, Authenticom [redacted].[64] In other words, Authenticom was [redacted].[65] Because Authenticom was [redacted], Authenticom's circumvention measures designed to complete its polling process are inextricably connected to the copyrighted material. Any nexus requirement is easily satisfied.

[63] The policy issues that concerned the *Chamberlain* court are also absent here. That case involved a device that allegedly violated the DMCA when it was used to open certain types of garage doors. These garage doors—including their operative software—were owned outright by consumers, who had full rights to copy, use, and access the software. *See Chamberlain*, 381 F.3d at 1193 ("[T]he copyright laws authorize consumers to use the copy of Chamberlain's software embedded in the GDOs that they purchased."). It is undisputed that the dealers do not own Reynolds software. *See, e.g.*, Ex. 2 at 63:22-64:2 (Kirby tr.).

[64] Ex. 39 at 30:5-31:6; 34:13-35:13; 37:3-17 (Munns tr.); Ex. 2 at 161:11-162:23 (Kirby tr.); Ex. 33, AUTH_00141204.

[65] Ex. 39 at 113:17-115:18 (Munns tr.); Ex. 34, AUTH_00093108 (stating that [redacted]).

B. Authenticom Violated the Wisconsin Computer Crime Statute.

Reynolds is also entitled to summary judgment on its claim that Authenticom's actions violated the Wisconsin Computer Crimes Act. The Computer Crimes Act makes it makes it unlawful to "willfully, knowingly and without authorization" (3) access "computer programs or supporting documentation" or (6) disclose "restricted access codes or other restricted access information to unauthorized persons." Wis. Stat. § 943.70(2)(a). The Computer Crimes Act is similar to yet broader than the federal Computer Fraud and Abuse Act ("CFAA")—among other things, the Computer Crimes Act encompasses "computer programs" in addition to "computers," does not require civil litigants to show "loss or damage," and covers unauthorized disclosure of access information. *See generally* Wis. Stat. § 943.70. Because of this, "entry of summary judgment in [a] plaintiff's favor on this claim is an even easier call than entry on the first element of [a] CFAA claim." *Epic Sys. Corp. v. Tata Consultancy Servs., Ltd.*, 14-cv-748-wmc, 2016 WL 4033276, at *23 (W.D. Wis. Jul. 27, 2016).

1. Authenticom acted "willfully, knowingly and without authorization."

The initial predicate for a Computer Crimes Act claim is that the defendant acted "willfully, knowingly and without authorization." Wis. Stat. § 943.70(2). This Court has already addressed the meaning of "without authorization" in the context of the CFAA, 18 U.S.C. § 1030. The Court held that the DMS provider's authorization—independent from a dealer's authorization—is required to access the DMS in question:

> The CFAA's phrase "without authorization" confirms that computer owners have the power to revoke the authorizations they grant. Thus, a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability.

Order at 14 [Dkt. 506] (internal marks omitted).[66] The Court recently reaffirmed that holding in rejecting the dealers' motion to dismiss CDK's counterclaims. Order at 19-20 [Dkt. 749]. That legal analysis applies here with equal effect: "unauthorized" within the meaning of the Computer Crimes Act means without the authorization of the owner of the computer program at issue.

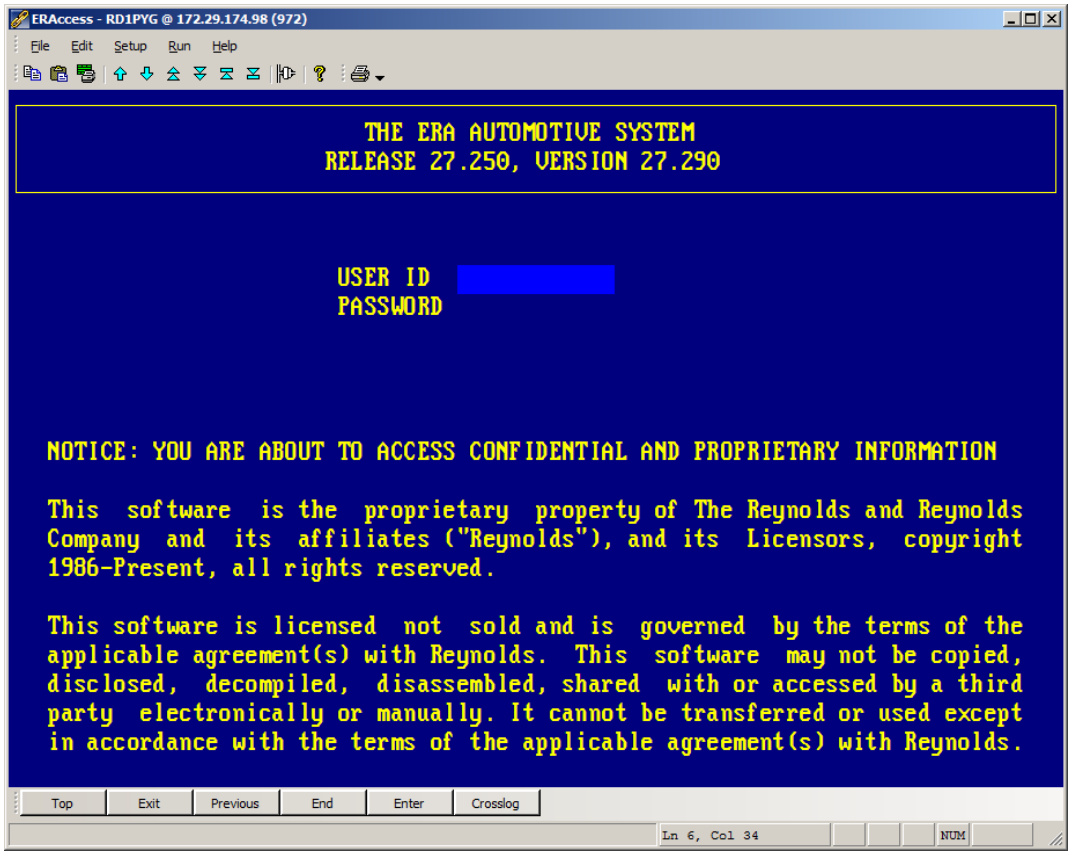
This analysis is confirmed by *Epic Systems Corp*., 2016 WL 4033276. Epic, a software services company, had a contract with non-party Kaiser Permanente that allowed Kaiser to access its online web portal. *Id.* at *3. An employee of one of Kaiser's consultants, Tata Consultancy, obtained credentials to this web portal, downloaded documents from the web portal, and provided his credentials to other Tata employees. *Id.* at *7-8. The Court granted partial summary judgment on the first element of Epic's CFAA claim, and all the elements of its Computer Crimes Act claim, on two independent grounds: that Tata had accessed documents from Epic's cloud web portal without authorization and had disclosed username credentials to non-authorized personnel. *Id.* at *23. The Court found that Tata acted without authorization even though Tata was a consultant of an authorized customer, Kaiser. *Id.* at *7, *23.

There can be no serious dispute that Authenticom knew that its access to the Reynolds DMS was unauthorized by Reynolds. Reynolds had informed the world since at least 2007 that it did not approve of third parties accessing its DMS.[67] Reynolds made repeated announcements to its customer base and the market that third-party access to its DMS was prohibited.[68]

---

[66] *See also* Order at 15 [Dkt. 506] ("[A]s Judge Easterbrook pointed out at the Seventh Circuit oral argument, the 'authorization' required for lawful access under the CFAA must come from the owner of the computer system, not from anyone who happens to use the system."); *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067 (9th Cir. 2016), cert. denied, 138 S. Ct. 313 (2017); *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1183 (N.D. Cal. 2013).
[67] *See, e.g.*, Ex. 97, REYMDL00015601 (Apr. 2007 Automotive News Article); Ex. 17 (Feb. 19, 2007 Automotive News Article); Ex. 98, REYMDL01075600 (Mar. 2012 Automotive News Article).
[68] *See, e.g.*, Ex. 18, REYMDL00022899 (Fuel Article Jan. 1, 2010: "It remains our policy to not allow 'hostile interfaces' or unauthorized code on your systems to protect both Reynolds and your dealership from security breaches and potential data corruption issues."); Ex. 108 (same).

As Authenticom's documents make clear, Reynolds backed those announcements with concrete enforcement steps, and Authenticom was well aware of Reynolds's policy.[69] Authenticom announced to its entire customer base in 2013 that Reynolds was [redacted]"[70] Authenticom's executives admitted that [redacted].[71] The ERA login screen[72] further announced Reynolds's prohibition on third-party access or use:



[69] *See, e.g.*, Ex. 93, REYMDL00015727; Ex. 26, AUTH_00468320; Ex. 83, AUTH_00472681 (noting that [redacted]"); Ex. 84, AUTH_00170766.

[70] Ex. 19, AUTH_00170940.

[71] Ex. 29 at 21:11-12 (Cottrell 2019 tr.) ("[redacted]"); *see also* Ex. 85 at 100:1-6; 128:14-16 (Gentry tr.) ("[redacted]"); Ex. 28 at 60:5-63:22 (Clements tr.) ([redacted]; Ex. 86, AUTH_00091619, at 621. Authenticom's CEO testified that Reynolds's view of Authenticom's DMS access "[redacted]" Ex. 29 at 270:10-19 (Cottrell 2019 tr.).

[72] Ex. 13.

Authenticom employees admitted [redacted].[73] Notwithstanding this clear notice, they uniformly testified that [redacted].[74]

Reynolds had also sued another "integrator," SIS, in federal court in 2012 for violating the CFAA and for other wrongful acts.[75] As Reynolds alleged in that complaint (and was later upheld by the court): "Under the Reynolds Customer Agreement, customers are prohibited from allowing third party integrators like SIS to interface with the ERA DMS."[76] Reynolds provided that ruling and the contractual language it was based upon to Authenticom.[77] And last but not least, Reynolds sent Authenticom its own express cease-and-desist letter in 2015, demanding that it cease accessing the Reynolds DMS.[78] In short, the record uncontrovertibly demonstrates that Authenticom was fully on notice that its accessing and use of the Reynolds DMS—absent specific permission from Reynolds—was not authorized.[79] Despite these repeated warnings, Authenticom continued to access the Reynolds DMS.[80] The Computer Crimes Act's scienter and authorization requirements are thus satisfied.

[73] *See, e.g.*, Ex. 87, AUTH_00175368; Ex. 88, AUTH_00472396; Ex. 89, AUTH_00155147; Ex. 39 at 351:13-356:19 (Munns tr.); Ex. 2 at 174:22-179:4 (Kirby tr.); Ex. 44 at 121:18-128:20 (Hembd tr.).
[74] *See* Ex. 28 at 99:22-103:16 (Clements tr.); Ex. 39 at 351:9-356:19, 360:4-21 (Munns tr.); Ex. 2 at 68:7-70:9; 163:13-167:16 (Kirby tr.); Ex. 44 at 121:11-16, 131:11-134:1 (Hembd tr.).
[75] Ex. 7, REYMDL00015586 ¶¶ 49-57. The court may take judicial notice of the fact of Reynolds's public filings in the 2012 litigation against SIS. *See Daniel v. Cook Cty.*, 833 F.3d 728, 742 (7th Cir. 2016) ("Courts routinely take judicial notice of the actions of other courts or the contents of filings in other courts.").
[76] *Id.* ¶ 11; *Reynolds & Reynolds Co. v. Superior Integrated Sols., Inc.*, 1:12-CV-848, 2013 WL 2456093, at *2 (S.D. Ohio June 6, 2013) ("Reynolds' auto-dealership customers agree to certain prohibitions on integration of third party applications when the customers license Reynolds' ERA. When they sign up for ERA, customers typically agree to prohibitions on connecting third-party applications to ERA. The customers also agree to prohibitions on allowing third-party integrators that are not licensed by Reynolds, like SIS, to interface with ERA.") (citations omitted).
[77] Ex. 90, AUTH_00468019.
[78] Ex. 91, REYMDL00012553.
[79] Authenticom's own complaint in this case admits these same basic facts. *See* Authenticom Compl. [Dkt. 1] ¶¶ 6, 92, 103, 106-107, 109, 185.
[80] *See, e.g.*, Ex. 39 at 360:4-10 (Munns tr.).

2. Authenticom accessed Reynolds's "computer programs."

The Computer Crimes Act defines "computer program" to mean "an ordered set of instructions or statements that, when executed by a computer, causes the computer to process data." Wis. Stat. § 943.70(c). The software that comprises the Reynolds DMS all readily satisfies this definition. ERAccess.exe and ERA-IGNITE.exe both constitute computer programs, as do the other software components that make up the DMS.[81] Authenticom's utilization of Reynolds's DMS when conducting automated data polling also incontrovertibly involved *accessing* Reynolds's computer programs—[redacted][82] Authenticom violated (and continues to violate) the Computer Crimes Act accordingly.

3. Authenticom also disclosed "restricted access codes or other restricted access information to unauthorized persons."

Authenticom also violated the Computer Crimes Act—an *even* "easier call," as the court in *Epic* put it— because the evidence is undisputed that Authenticom disclosed Reynolds's DMS credentials to unauthorized individuals (namely, Authenticom employees). *Epic Sys. Corp.*, 2016 WL 4033276, at *23 ("Even if there were disputed facts as to this prong, there is no dispute that TCS employee Gajaram disclosed his UserWeb credentials to other TCS employees, none of whom were authorized to access the UserWeb."); *Burbank Grease Services, LLC v. Sokolowski*, 717 N.W.2d 781, 795 (Wis. 2006) (statute "prohibits the unauthorized disclosure of codes, passwords or other information that grants access to restricted-access systems"). Authenticom has admitted that it used dealer log-in credentials to access Reynolds's DMS.[83] The evidence is also

[81] Auth. P.I. Tr. 2-P [Auth. Dkt. 163] at 14 (Testimony of R. Schaefer); Declaration of R. Schaefer [Auth. Dkt. 97] ¶¶ 4, 14, 27; Auth. Resp. to DSAF [Auth. Dkt. 24] ¶¶ 24, 58.
[82] *See, e.g.*, Ex. 39 at 30:5-31:6, 34:13-35:13, 37:3-17, 113:17-115:18 (Munns tr.); Ex. 2 at 161:11-162:23 (Kirby tr.); Ex. 33, AUTH00141204; Ex. 34, AUTH_00093108.
[83] *See, e.g.*, Ex. 45 at 68:7-8 (Robinson tr.) ([redacted]"); Ex. 29 at 184:7-12 (Cottrell 2019 tr.) ([redacted]). [redacted]. Ex. 29 at 197:20-198:1 (Cottrell 2019 tr.) (when Authenticom

clear that [redacted].[84] Authenticom [redacted]

[redacted].[85] There can be no doubt on this record that Authenticom violated the Computer Crimes Act.

VI. Conclusion

For the reasons set forth above, and based on the facts and evidence set forth in Reynolds's accompanying Statement of Material Undisputed Facts, Reynolds asks the Court to enter a partial summary judgment holding that:

1. Authenticom's efforts to circumvent Reynolds's DMS access controls—namely, Reynolds's CAPTCHA prompts and Reynolds Suspicious User ID measure—violated 17 U.S.C. § 1201(a)(1).

2. Authenticom's accessing of Reynolds's computer programs without Reynolds's authorization violated the Computer Crimes Act.

3. Authenticom's disclosure of Reynolds DMS credentials violated the Computer Crimes Act.

[Signature block on following page]

[redacted]"; *id.* at 199:18-200:6 (Authenticom [redacted]").

[84] *See, e.g.*, Ex. 24 at 64:18-22 (Wiersgalla tr.) ("[redacted]"); Ex. 45 at 72:7-13 (Robinson tr.) ([redacted].

[85] *See, e.g.*, Ex. 41, AUTH_0043125); Ex. 42, AUTH_00431361; Ex. 43, AUTH_00170533; Ex. 103, AUTH_00170330; Ex. 104, AUTH_00169111; Ex. 105, AUTH_00195650; Ex. 106, AUTH_00230497; Ex. 28 at 151:24-153:6 (Clements tr.) ([redacted]).

Dated: October 15, 2019

Respectfully submitted,

/s/ *Aundrea K. Gulley*

Aundrea K. Gulley
Brian T. Ross
Brice A. Wilkinson
Ross A. MacDonald
GIBBS & BRUNS LLP
1100 Louisiana Street
Suite 5300
Houston, TX 77002
(713) 751-5258
agulley@gibbsbruns.com
bross@gibbsbruns.com
bwilkinson@gibbsbruns.com
rmacdonald@gibbsbruns.com

Michael P.A. Cohen
Leo D. Caseria
SHEPPARD MULLIN RICHTER & HAMPTON, LLP
2099 Pennsylvania Avenue NW, Suite 100
Washington, DC 20006
(202) 747-1900
mcohen@sheppardmullin.com
lcaseria@sheppardmullin.com

Counsel for Defendant
The Reynolds and Reynolds Company

CERTIFICATE OF SERVICE

I, Brice A. Wilkinson, an attorney, hereby certify that on October 15, 2019, I caused a true and correct copy of the foregoing **COUNTERCLAIMANT THE REYNOLDS AND REYNOLDS COMPANY'S [PROPOSED] MEMORANDUM IN SUPPORT OF ITS MOTION FOR PARTIAL SUMMARY JUDGMENT** to be filed and served electronically via the court's CM/ECF system. Notice of this filing will be sent by e-mail to all parties at the following email address: SERVICE-EXTERNAL-DMS-MDL@lists.kellogghansen.com.

/s/ Brice A. Wilkinson
Brice A. Wilkinson
GIBBS & BRUNS LLP
1100 Louisiana Street
Suite 5300
Houston, TX 77002
(713) 751-5218
bwilkinson@gibbsbruns.com